

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)
 Ryota AKIYAMA, et al.) Group Art Unit: To Be Assigned
 Serial No.: To Be Assigned) Examiner: To Be Assigned
 Filed: September 24, 1999)
 For: AUTHENTICATION SYSTEM,)
 AUTHENTICATION METHOD,)
 SIGNING APPARATUS,)
 SIGNING METHOD, CERTIFYING)
 APPARATUS, CERTIFYING)
 METHOD, AND A COMPUTER-)
 READABLE RECORDING MEDIUM)
 WITH A PROGRAM MAKING A)
 COMPUTER EXECUTE THE)
 METHOD RECORDED THEREIN)



**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
 APPLICATION IN ACCORDANCE
 WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Assistant Commissioner for Patents
 Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-088233, filed March 30, 1999.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY

Dated: September 24, 1999

By:

James D. Halsey, Jr.
 Registration No. 22,729

700 Eleventh Street, N.W., Suite 500
 Washington, D.C. 20001
 (202) 434-1500

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

1999年 3月30日

願 番 号
Application Number:

平成11年特許願第088233号

願 人
Applicant(s):

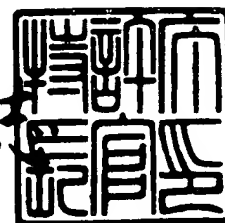
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 4月30日

特許庁長官
Commissioner,
Patent Office

伴佐山 建



出証番号 出証特平11-3026948

【書類名】 特許願

【整理番号】 9950331

【提出日】 平成11年 3月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 認証装置および記録媒体

【請求項の数】 6

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 秋山 良太

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小谷 誠剛

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 長谷部 高行

【発明者】

【住所又は居所】 東京都港区芝浦四丁目15番33号 株式会社富士通ビー・エス・シー内

【氏名】 佐々木 孝興

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089141

【住所又は居所】 東京都目黒区平町1丁目21番20-603号

【弁理士】

【氏名又は名称】 岡田 守弘

【電話番号】 03-3725-2215

【手数料の表示】

【予納台帳番号】 015543

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705795

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証装置および記録媒体

【特許請求の範囲】

【請求項 1】

情報を鍵を用いて一方向性の関数で認証子を作成して署名する認証装置において、

情報を複数のデータに分割する手段と、

上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、

上記作成したそれぞれの認証子を上記情報に結合する手段とを備えたことを特徴とする認証装置。

【請求項 2】

情報を鍵を用いて一方向性の関数で認証子を作成して署名する認証装置において、

情報を複数のデータに分割する手段と、

上記分割した 1 つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、

上記作成したそれぞれの認証子を上記情報に結合する手段とを備えたことを特徴とする認証装置。

【請求項 3】

情報を鍵を用いて一方向性の関数で認証子を作成して検証する認証装置において、

情報からデータと認証子を分離する手段と、

上記分離した情報を複数のデータに分割する手段と、

上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、

上記作成したそれぞれの認証子および上記分離したそれぞれの認証子をもとに

検証する手段と

を備えたことを特徴とする認証装置。

【請求項 4】

情報を鍵を用いて一方向性の関数で認証子を作成して検証する認証装置において、

情報からデータと認証子を分離する手段と、

上記分離した情報を複数のデータに分割する手段と、

上記分割した 1 つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、

上記作成したそれぞれの認証子および上記分離した認証子をもとに検証する手段と

を備えたことを特徴とする認証装置。

【請求項 5】

情報を複数に分割する手段と、

上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、

上記作成したそれぞれの認証子を上記情報に結合する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項 6】

情報を複数に分割する手段と、

上記分割した 1 つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、

上記作成したそれぞれの認証子を上記情報に結合する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報を鍵を用いて一方向性の関数で認証子を作成して署名および検証する認証装置および記録媒体に関するものである。

【0 0 0 2】

【従来の技術】

従来、文字、数字、記号列で作成される文書（ドキュメント）の偽造を防止するために、当該文書を所定ブロックに分割して一方向性の関数（例えばハッシュ関数）を用いて認証子を作成し、文書中の数字を他の数字に変更するというような、偽造を防止するようにしていた。

【0 0 0 3】

【発明が解決しようとする課題】

しかしながら、上述した従来の一方向性の例えばハッシュ関数を用いて認証子を作成するシステムでは、偽造をより困難にするにはハッシュ関数の処理ブロック長を長くする手法が用いられていたが、十分な偽造が防止し得ないという問題があった。即ち、従来のハッシュ関数では、AND 論理、OR 論理の他四則演算子等を複雑に組み合わせて一方向性関数を実現していたが、これは経験的・直感的手法に基づいて行われ、組織的な構成法によらない。このため、従来のハッシュ関数の中には、正当なデータをハッシュ処理して得た署名データ（認証子）を不当データに改ざんして同様にハッシュ処理した結果が一致するいわゆる署名偽造が起こる問題があった。

【0 0 0 4】

本発明は、これらの問題を解決するため、情報を複数に分割して異なる鍵を用い任意の信頼できる一方向性関数でそれぞれ認証子を作成して結合し、偽造情報作成確率を低減することを目的としている。

【0 0 0 5】

【課題を解決するための手段】

図 1 を参照して課題を解決するための手段を説明する。

図 1 において、ハッシュ手段 2 は、鍵を用いて一方向性の関数で認証子を作成

するものである。

【 0 0 0 6 】

結合手段 5 は、認証子とデータを結合するものである。

分離手段 7 は、情報からデータと認証子とを分離するものである。

比較手段 8 は、情報から分離した認証子と、情報から作成した認証子とを比較するものである。

【 0 0 0 7 】

次に、動作を説明する。

ハッシュ手段 2 が情報から分割した各データについてそれぞれの鍵 3 を用いて一方向性の関数でそれぞれの認証子を作成し、結合手段 5 が作成したそれぞれの認証子を情報に結合するようにしている。

【 0 0 0 8 】

また、ハッシュ手段 2 が情報から分割した 1 つのデータについて鍵 3 を用いて一方向性の関数で認証子を作成および一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵 3 を用いて一方向性の関数で認証子を作成することを繰り返し、結合手段 5 が作成したそれぞれの認証子を情報に結合するようにしている。

【 0 0 0 9 】

また、分離手段 7 が情報からデータと認証子を分離し、ハッシュ手段 2 が分離された情報を複数に分割した各データについてそれぞれの鍵 3 を用いて一方向性の関数でそれぞれの認証子を作成し、比較手段 8 が作成したそれぞれの認証子および分離したそれぞれの認証子をもとに検証するようにしている。

【 0 0 1 0 】

また、分離手段 7 が情報からデータと認証子を分離し、分離された情報を複数に分割した 1 つのデータについて鍵 3 を用いて一方向性の関数で認証子を作成および一方向性の関数で認証子 4 を作成する際の中間の任意のデータと次のデータについて鍵 3 を用いて一方向性の関数で認証子作成することを繰り返し、比較手段 8 が作成したそれぞれの認証子および分離した認証子をもとに検証するようにしている。

【0 0 1 1】

従って、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合したり、情報から分離した認証子と情報から分離したデータを分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して検証したりすることにより、偽造情報作成確率を低減することが可能となる。

【0 0 1 2】

【実施例】

次に、図 1 から図 6 を用いて本発明の実施の形態および動作を順次詳細に説明する。ここでは、以下、情報（テキスト、画像（静止画、動画）、音声などからなる情報）中の文（テキスト）を例に具体的に説明する（以下の具体的な説明は、例であって、画像（静止画、動画）、音声などの全てについて同様に適用できるものである）。

【0 0 1 3】

図 1 は、本発明のシステム構成図を示す。

図 1 において、署名側は、左側の半分によって構成され、認証子を作成して文に結合するものである。

【0 0 1 4】

検証側は、右側の半分によって構成され、文から認証子を分離して文から作成した認証子とを比較して検証するものである。

データ 1 は、文から分割したデータ D 1 ないし D n であって、後述する図 5 の文（ドキュメント）中の数字、文字、記号などを所定ブロック毎に分割したデータ D 1 から D n である。

【0 0 1 5】

ハッシュ手段 2 は、データ D 1 ないし D n についてそれぞれの鍵 K 1 から K m を用いて一方向性の関数でそれぞれの認証子 C S 1 から C S m をそれぞれ作成するものである。

【0 0 1 6】

鍵 3 は、認証子 C S 1 から C S m を作成するそれぞれの鍵である。

認証子 4 は、鍵 K 1 から K m によって作成されたそれぞれの認証子である。

結合手段 5 は、作成した認証子 4 と、データ D 1 から D n とを結合するものであって、後述する図 5 のドキュメント例に示すように、認証子 4 を下段に付加などするものである。

【0017】

分離手段 7 は、文からデータ D 1' から D n'、および認証子 4 を分離するものである。

比較手段 8 は、文から分離した認証子と、文から作成した認証子とを比較し、例えば一致したときに文が偽造されていなく真正と認証するものである。

【0018】

次に、図 1 の構成の動作を説明する。

(1) 署名側における認証子の作成：

(1-1) 文を複数に分割した入力データ D 1 から D n 毎に、それぞれの鍵を用いてハッシュ手段 2 が認証子 4 である C S 1 から C S m を作成する。

【0019】

(1-2) 作成された C S 1 から C S m と、データ D 1 から D n とを結合する。例えば後述する図 5 のドキュメント（文）に示すように、文章中の下段に認証子（例えば 1 桁 4 ビットからなる 8 桁分の認証子）を付加する。

【0020】

以上によって、文を分割したデータ D 1 から D n 毎にそれぞれの鍵を用いて認証子 C S 1 から C S m を作成し、データ D 1 から D n に結合することにより、文を分割したデータ D 1 から D n 毎に異なる鍵を用いて認証子を作成することで偽造文の作成を極めて困難にし信頼性を大幅に向上させることが可能となる。

【0021】

(2) 検証側における認証子の作成：

(2-1) (1) で作成された図 5 の文（ドキュメント）から認証子 C S 1 から C S m とデータ D 1' から D n' を分離する。

【0022】

(2-2) 分離したデータ D 1' から D n' 毎に、それぞれの鍵を用いてハッシュ手段 2 が認証子 4 である C S 1' から C S m' を作成する。

(2-2) 作成されたCS1'からCSm'と、分離された認証子CS1からCSmとを比較し、一致するか判別し、一致したときに真正の文であって偽造されていないと判定する。一方、1つでも一致しないときは偽造された文と判定する。

【0023】

以上によって、文から分離したデータD1からDn毎にそれぞれの鍵を用いて認証子CS1'からCSm'を作成し、分離した認証子CS1からCSmとを比較して全て一致したときに真正の文と判定し、1つでも不一致のときに偽造された文と判定することにより、文を分割したデータD1からDnについて異なる複数の鍵を用いて認証子をそれぞれ作成して結合することで偽造文の作成を極めて困難にし信頼性を大幅に向上させることが可能となる。以下順次詳細に説明する。

【0024】

図2は、本発明の1実施例構成図（独立多並列）を示す。これは、文を分割した入力データD1からDnについて、m並列にそれぞれの鍵を用いてハッシュ手段2により認証子CS1からCSmを並列に同時に作成するときの構成を示す。

【0025】

図2の(a)は、構成図を示す。

図2の(a)において、入力データD1からDnは、文を分割したデータD1からDnである。

【0026】

ハッシュ手段2は、鍵Kを用いて認証子CSを作成するものであって、ここでは、EOR21、一方向性関数（例えばハッシュ関数）22およびトランケート23から構成されるものである（図3の(b)を用いて後述する）。

【0027】

EOR21は、排他論理和演算を実行するものであって、ここでは、データと前回の一方向性関数22で求めた値（初回は初期値IV）との排他論理和演算を行うものである。

【0028】

一方向性関数（一方向性関数器）22は、鍵Kをもとに、EOR21によって演算したデータから一方向性関数（例えばハッシュ関数）によって不可逆性の認証子CSを作成するものである。

【0029】

トランケート23は、一方向性関数22によって作成された認証子CSを出力するものである。

出力データ（D1からDn, CS1からCSm）は、入力データD1からDnについて作成した認証子CS1からCSmを結合したものである（図5参照）。

【0030】

図2の（b）は、認証子CSの生成プロセスを示す。

図2の（b-1）は、CS1の生成プロセスを示す。

図2の（b-1）において、

①IV=公開定数：これは、図2の（a）の左側から1番目のハッシュ手段2を構成するEOR21に初期値IVを設定する。

【0031】

②EK1[IV (+) D1]=L11：これは、図2の（a）のEOR21が①で設定した初期値IVと、1番目のデータD1とを排他論理和演算し、その排他論理和演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算（例えばハッシュ関数によって演算）して値L11を得る。

【0032】

③EK1[L11 (+) D2]=L12：これは、図2の（a）のEOR21が②で得た値L11と、2番目のデータD2とを排他論理和演算し、その排他論理和演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算（例えばハッシュ関数によって演算）して値L12を得る。

【0033】

④EK1[L1(n-1) (+) Dn]=L1n：これは、同様にして、図2の（a）のEOR21が前回に得た値L1(n-1)と、n番目のデータDnとを排他論理和演算し、その排他論理和演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算（例えばハッシュ関数によって演算）して値L1

nを得る。

【0 0 3 4】

⑤ $Tr[L1n] = CS1$: これは、最後の n 番目のデータ Dn まで終了したので、最後の n 番目の演算結果 $L1n$ を認証子 $CS1$ として出力する。

以上の①から⑤の手順によって、鍵 $K1$ 、初期値 IV を用いて認証子 $CS1$ を作成することが可能となる。

【0 0 3 5】

図 2 の (b-2)、(b-3) は、図 2 の (b-1) の①から⑤の手順と同様に、認証子 $CS2$ 、 $CS3$ を求める様子を示す。これを続けて認証子 CSm を同様に求める。

【0 0 3 6】

以上のように、独立に m 並列で鍵 $K1$ から Km をそれぞれ用いて同時に認証子 $CS1$ から CSm を算出することが可能となる。ここでは、 CSm 個あたりの偽造確率 $= 1 / 2^{mP}$ (P は認証子のビット長) となり、認証子 CS の数を増やすことで偽造確率を小さくすることができると共に、並列処理ができ CS の数に依存しないで同一時間で処理可能となる。

【0 0 3 7】

次に、図 3 を用いて図 2 の $m = 3$ (独立 3 並列) の場合の構成と動作を詳細に説明する。

図 3 は、本発明の具体例構成図 (独立 3 並列) を示す。

【0 0 3 8】

図 3 の (a) は、独立 3 並列の構成図を示す。これは、図 2 において、 $m = 3$ とした場合の例であって、ハッシュ手段 2、 $EO R 21$ 、一方向性関数 22、およびトランケート 23 は、図 2 の同一番号のものと同一であるので、説明を省略する。

【0 0 3 9】

図 3 の (b) は、ハッシュ手段 2 における $CS1$ から $CS3$ の生成プロセスを示す。

図 3 の (b-1) は、図 3 の (a) の入力データ $D1$ から Dn 、鍵 $K1$ 、初期

値 IV をもとに認証子 $CS1$ を作成するときの手順を示す。

【0040】

図3の(b-1)において、

①' $IV = \text{公開定数}$: これは、図3の(a)の左側から1番目のハッシュ手段2を構成する $EOR21$ に初期値 IV を設定する。

【0041】

②' $EK1[IV(+)D1] = L11$: これは、図3の(a)の $EOR21$ が①' で設定した初期値 IV と、1番目のデータ $D1$ とを排他論理和演算し、その排他論理和演算した値について、一方向性関数22が鍵 $K1$ を用いて一方向性の演算(例えばハッシュ関数によって演算)して値 $L11$ を得る。

【0042】

③' $EK1[L11(+)D2] = L12$: これは、図3の(a)の $EOR21$ が②' で得た値 $L11$ と、2番目のデータ $D2$ とを排他論理和演算し、その排他論理和演算した値について、一方向性関数22が鍵 $K1$ を用いて一方向性の演算(例えばハッシュ関数によって演算)して値 $L12$ を得る。

【0043】

④' $EK1[L1(n-1)(+)Dn] = L1n$: これは、同様にして、図3の(a)の $EOR21$ が前回に得た値 $L1(n-1)$ と、 n 番目のデータ Dn とを排他論理和演算し、その排他論理和演算した値について、一方向性関数22が鍵 $K1$ を用いて一方向性の演算(例えばハッシュ関数によって演算)して値 $L1n$ を得る。

【0044】

⑤' $Tr[L1n] = CS1$: これは、最後の n 番目のデータ Dn まで終了したので、最後の n 番目の演算結果 $L1n$ を認証子 $CS1$ として出力する。

図3の(b-2)、(b-3)は、図3の(b-1)の①' から⑤' の手順と同様に、認証子 $CS2$ 、 $CS3$ を求める様子を示す。

【0045】

以上の①' から⑤' の手順によって、独立に m 並列で鍵 $K1$ から $K3$ をそれぞれ用いて同時に認証子 $CS1$ から $CS3$ を算出することが可能となる。

次に、図 4 を用いて $m = 3$ で前段の中間データを次段の初期値とする場合の構成と動作を詳細に説明する。

【0046】

図 4 は、本発明の他の具体例構成図 ($m = 3$) を示す。

図 4 の (a) は、 $m = 3$ の構成図を示す。これは $m = 3$ として前段の中間データを次段の初期値とした場合の例であって、ハッシュ手段 2、EOR 21、一方方向性関数 22、およびトランケート 23 は、図 2 の同一番号のものと同じ（初期値のみことなる）であるので、説明を省略する。

【0047】

図 4 の (b) は、ハッシュ手段 2 における CS1 から CS3 の生成プロセスを示す。

図 4 の (b-1) は、図 4 の (a) の左から 1 番目のハッシュ手段 2 で CS1 を求める手順を示す。ここでは、既述した図 3 の (b-1) の①' から⑤' と同様にして CS1 を求める。

【0048】

図 4 の (b-2) は、図 4 の (a) の左から 2 番目のハッシュ手段 2 で CS2 を求める手順を示す。ここでは、前段の⑥に示す中間結果 ($L1(n-1)$) を初期値とし、既述した図 3 の (b-1) の①' から⑤' と同様にして CS2 を求める。

【0049】

図 4 の (b-3) は、図 4 の (a) の左から 3 番目のハッシュ手段 2 で CS3 を求める手順を示す。ここでは、前段の⑦に示す中間結果 ($L2(n-1)$) を初期値とし、既述した図 3 の (b-1) の①' から⑤' と同様にして CS3 を求める。

【0050】

以上の手順によって、 $m = 3$ で鍵 K1 から K3 をそれぞれ用いて前段の中間結果を次段の初期値として認証子 CS1 から CS3 を順次算出し、より信頼性を向上させることが可能となる。

【0051】

図 5 は、本発明の文の例を示す。ここでは、文（ドキュメント）は、例えば図示のように、文字、数字、記号などから構成され、これらを任意数毎にブロックに分割してデータ D 1 から D n を作成している。また、データ D 1 から D n よりそれぞれの鍵 K 1 から K m で作成した認証子 C S 1 から C S m を結合してドキュメントの下段の特定位置に 8 桁（1 桁 4 ビット）の認証子列を付加している。

【0052】

図 6 は、概念説明図を示す。

図 6 の（a）は本発明の概念説明図を示し、図 6 の（b）は従来技術の概念説明図を示す。

【0053】

図 6 の（b）において、文空間 M は偽造対象の文の取りうる仮想的な空間であり、認証子空間は認証子の取りうる仮想的な空間である。文空間 M 上で偽造をより防止するには、従来では、図示のように、認証子を長ブロックにして偽造確率を小さくしていた（認証子空間上で同じ値となる、文空間 M 上での偽造文空間 M 2 を点線から実線の円に示すように小さくしていた）。

【0054】

図 6 の（a）において、鍵 K 1 を用いた場合の文空間 M 上での偽造文空間 M 1、鍵 K 2 を用いた場合の文空間 M 上での偽造文空間 M 2、鍵 K 3 を用いた場合の文空間 M 上での偽造文空間 M 3 とすれば、本発明における鍵 K 1、K 2、K 3 の 3 つを用いた場合には、偽造空間 M 1、M 2、M 3 の共通領域である非常に小さな偽造空間 M 1 2 3 となり、偽造確率を大幅に小さくすることが可能となる。

【0055】

【発明の効果】

以上説明したように、本発明によれば、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合したり、情報から分離した認証子と情報から分離したデータを分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して検証したりする構成を採用しているため、偽造情報作成確率を簡易な手法で低減できると共に、並列処理により認証子作成時間を増やすことなく偽造情報確率を小さくしたり、前段の認証子作成時の任意の中間データを次

段の初期値などとして使用することで更に偽造確率を小さくしたりできる。

【図面の簡単な説明】

【図 1】

本発明のシステム構成図である。

【図 2】

本発明の 1 実施例構成図（独立多並列）である。

【図 3】

本発明の具体例構成図（独立 3 並列）である。

【図 4】

本発明の多の具体例構成図（ $m = 3$ ）である。

【図 5】

本発明の文の例である。

【図 6】

概念説明図である。

【符号の説明】

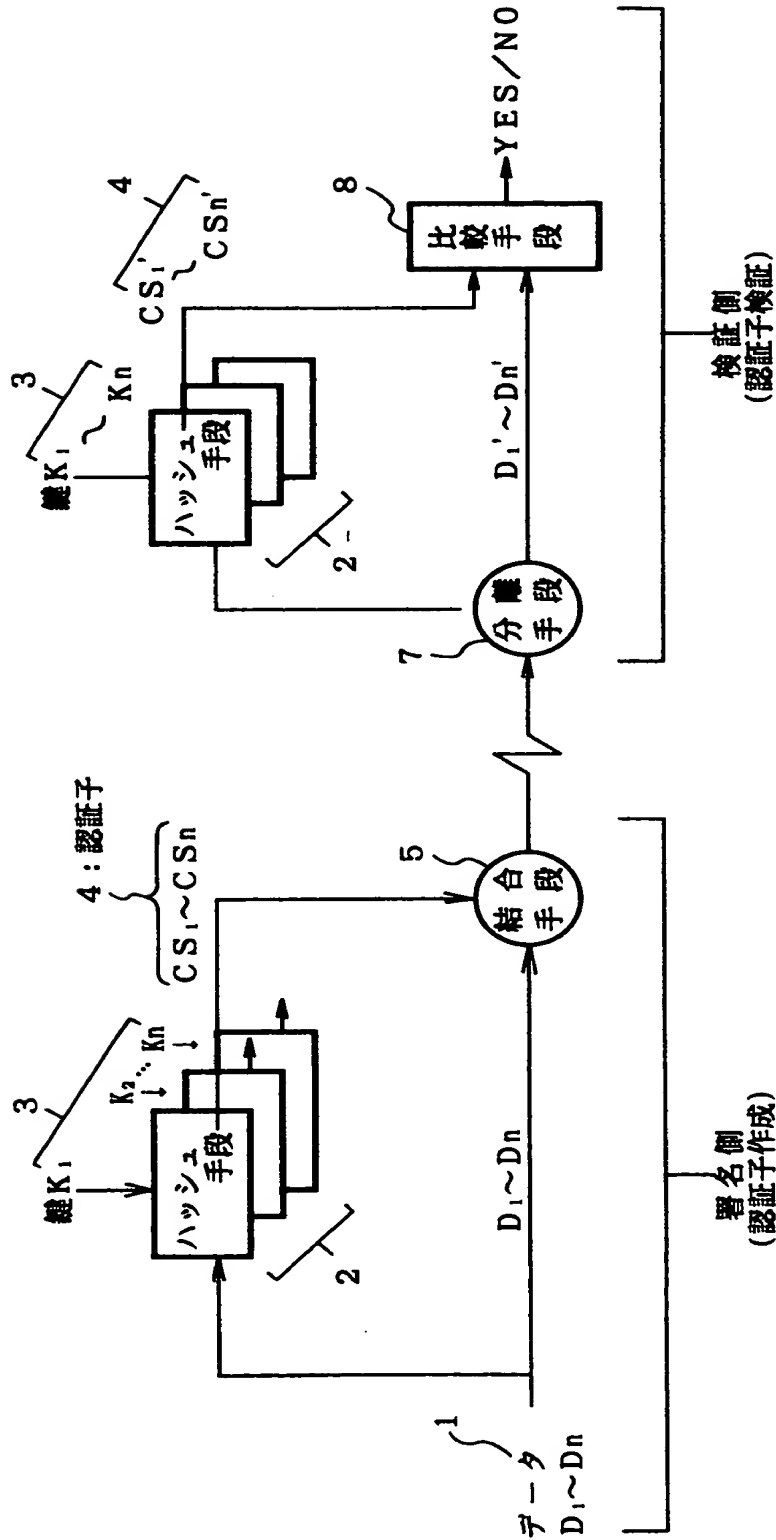
- 1 : データ
- 2 : ハッシュ手段
- 3 : 鍵
- 4 : 認証子
- 5 : 結合手段
- 7 : 分離手段
- 8 : 比較手段
- 2 1 : E O R（排他論理和演算器）
- 2 2 : 一方向性関数器
- 2 3 : トランケート

【書類名】

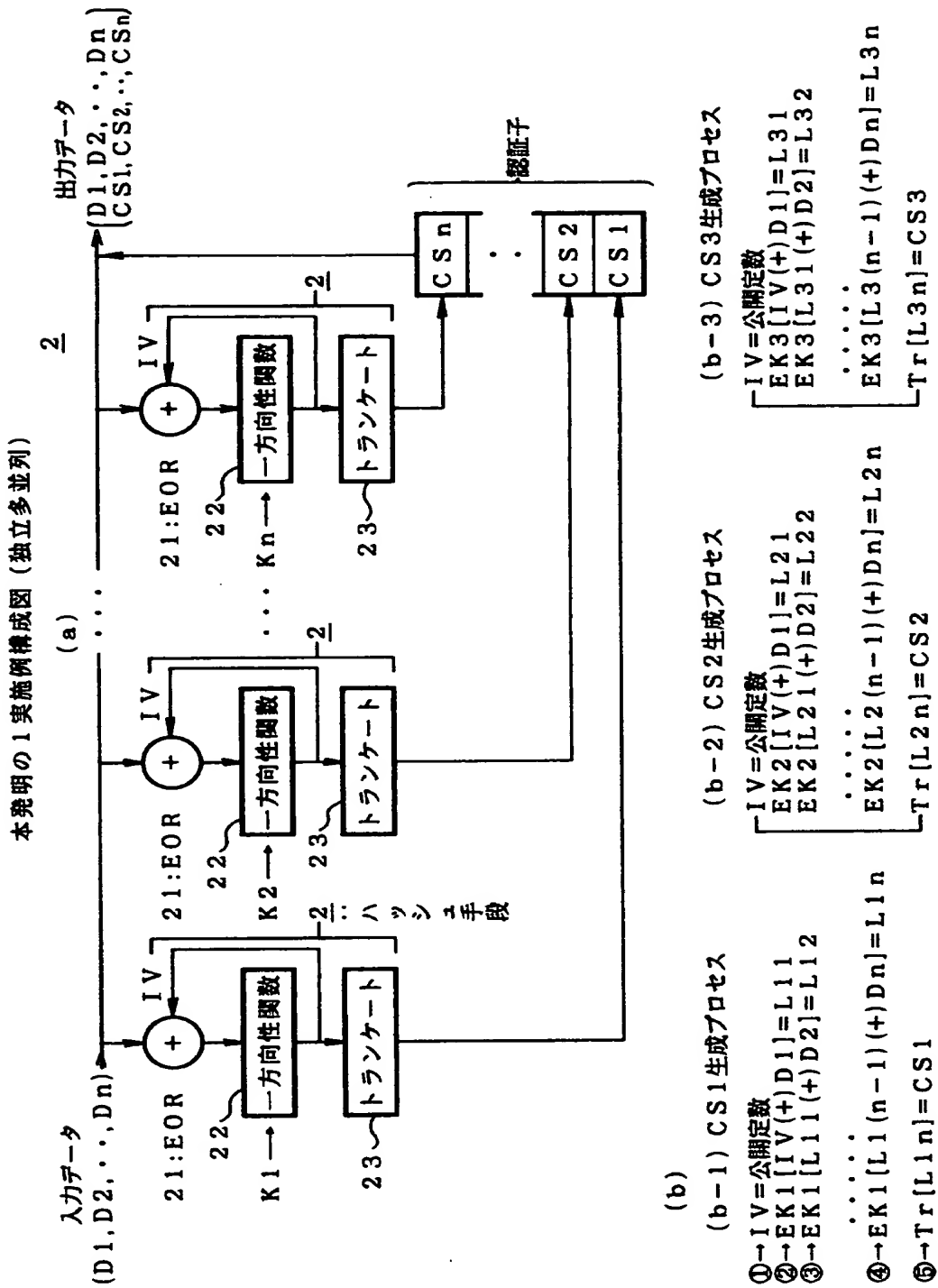
図面

【図 1】

本発明のシステム構成図

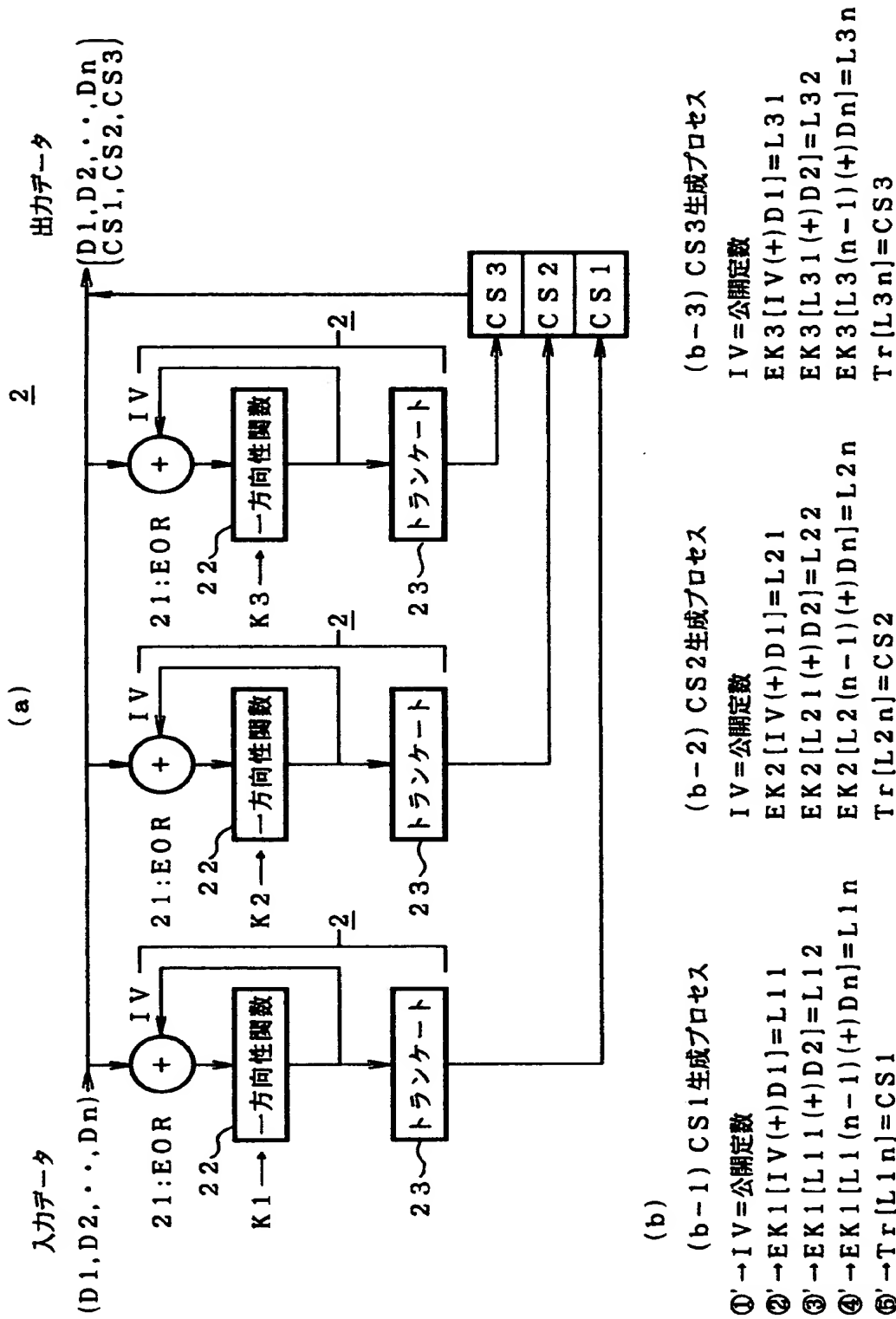


【図 2】

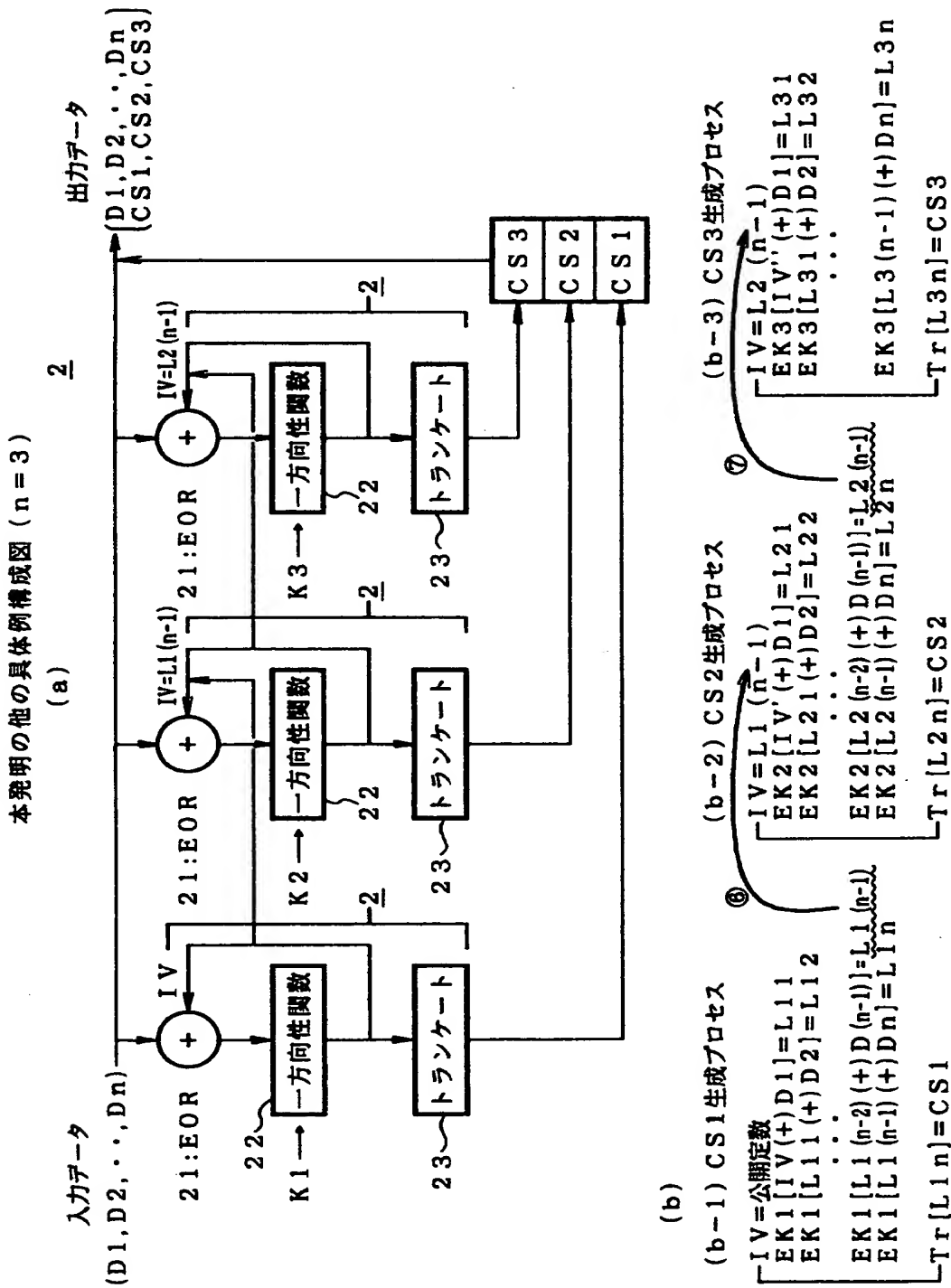


【図 3】

本発明の具体例構成図（独立 3 並列）



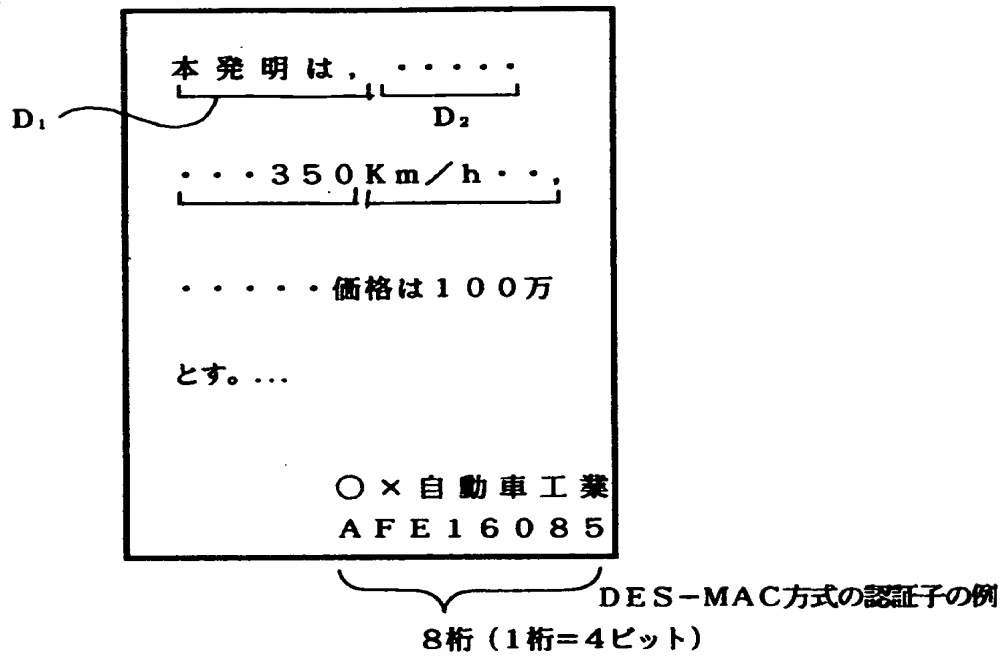
【図 4】



【図 5】

本発明の文の例

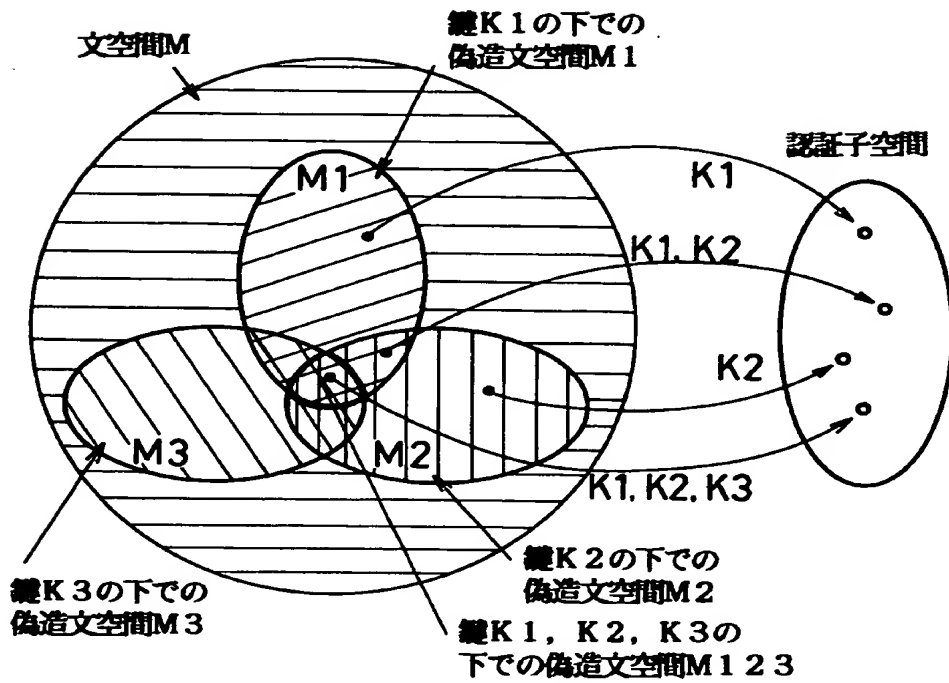
ドキュメントの一例



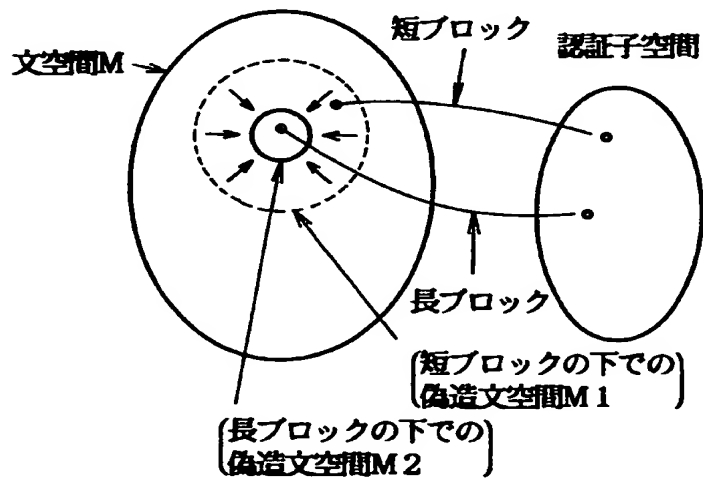
【図 6】

概念説明図

(a) 本発明



(b) 従来



【書類名】 要約書

【要約】

【課題】 本発明は、情報を鍵を用いて一方向性の関数で認証子を作成して署名および検証する認証装置および記録媒体に関し、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合などし、偽造情報作成確率を低減することを目的とする。

【解決手段】 情報を複数のデータに分割する手段と、分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、作成したそれぞれの認証子を情報に結合する手段とを備えるように構成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 2 2 3]

1. 変更年月日 1 9 9 6 年 3 月 2 6 日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名 富士通株式会社